

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-187511

(43)Date of publication of application : 08.07.1994

(51)Int.Cl. G06K 17/00
B42D 15/10
B42D 15/10
G09C 1/00
G11B 7/00
G11B 20/10

(21)Application number : 04-356116

(71)Applicant : OMRON CORP

(22)Date of filing : 18.12.1992

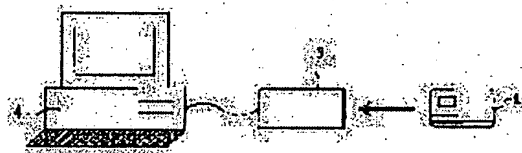
(72)Inventor : YODA SHIGERU
KITAJIMA HIROSHI
KOSHIBA YOSHIHITO

(54) INFORMATION RECORDING AND REPRODUCING SYSTEM

(57)Abstract:

PURPOSE: To record even such data for requiring the security on an optical IC card by providing a ciphering key on the IC part of the card when the information is recorded and reproduced at the optical recording part of the card.

CONSTITUTION: The information to be recorded is supplied to the IC part of an IC optical card 1 from a personal computer 4 via an optical IC card reader/ writer 5. The information is ciphered in the card 1 and the information acquired by this ciphering is sent to the reader/writer 5 and the ciphered information is written in the optical recording part of the card 1. The information is ciphered by the secret key of the IC part included in the card 1. Since this key is not viewed from an outside, the ciphered information can be decoded unless only when the secret key is used. The data recorded on the card 1 are read by the computer 4 when the card 1 is put into the reader/writer 5. Then the read information is decoded by the key of the IC part of the card 1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-187511

(43)公開日 平成6年(1994)7月8日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 K 17/00	A	7459-5L		
B 4 2 D 15/10	5 1 1	9111-2C		
	5 2 1	9111-2C		
G 0 9 C 1/00		8837-5L		
G 1 1 B 7/00	E	9195-5D		

審査請求 未請求 請求項の数7(全 6 頁) 最終頁に続く

(21)出願番号 特願平4-356116

(22)出願日 平成4年(1992)12月18日

(71)出願人 000002945

オムロン株式会社

京都府京都市右京区花園土堂町10番地

(72)発明者 余田 茂

京都府京都市右京区花園土堂町10番地 オムロン株式会社内

(72)発明者 北島 博史

京都府京都市右京区花園土堂町10番地 オムロン株式会社内

(72)発明者 小柴 美仁

京都府京都市右京区花園土堂町10番地 オムロン株式会社内

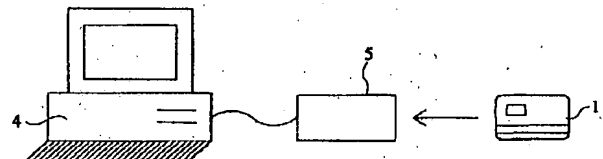
(74)代理人 弁理士 稲本 義雄

(54)【発明の名称】 情報記録再生システム

(57)【要約】

【目的】 守秘性を要求されるデータも光カードに記録できるようにする。

【構成】 光ICカード1のIC部3に暗号化鍵を記憶させ、その光ICカードをICカードリーダライタ5に挿入するとその暗号化鍵がパーソナルコンピュータ4によって読取られ、情報がその暗号化鍵によって暗号化され、光ICカード1に記録される。



【特許請求の範囲】

【請求項1】 光ICカードを使用した情報記録再生システムにおいて、

前記光ICカードの光記録部に記録再生する際の暗号化の鍵をそのカードのIC部に持つことを特徴とする情報記録再生システム。

【請求項2】 請求項1に記載の光ICカードを使用した情報記録再生システムにおいて、暗号化の鍵を前記光ICカードをアクセスする情報記録再生装置内に持つことを特徴とする情報記録再生システム。

【請求項3】 請求項1または請求項2に記載の光ICカードを使用した情報記録再生システムにおいて、前記光ICカード内の暗号化鍵と同じ暗号化鍵をアプリケーション提供者側のシステムに有することを特徴とする情報記録再生システム。

【請求項4】 請求項1乃至請求項3において、光記録部にセキュリティレベルを持ち、そのセキュリティレベルのうち少なくとも一部は情報を記憶する光ICカードに有する暗号化鍵とは別の鍵によってのみ再生できることを特徴とする情報記録再生システム。

【請求項5】 請求項4において、セキュリティレベルの一部をアクセスする別の鍵がICカードに記録されていることを特徴とする情報記録再生システム。

【請求項6】 請求項4において、セキュリティレベルの一部をアクセスする別の鍵が受動的な外部記憶メディアに記録されていることを特徴とする情報記録再生システム。

【請求項7】 請求項4において、セキュリティレベルの一部をアクセスする別の鍵が光ICカードまたは情報が記録される光ICカードとは別の光ICカードであることを特徴とする情報記録再生システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、光カードに情報を記録あるいは再生する情報記録再生システムに関する。

【0002】

【従来の技術】 光ICカードはクレジットカード大の形状をしており、そこに光記録部とIC部を備えている。光記録部は2.8MB程度のデータが記録できるようになっており、記録したデータは消去できないようになっている。一方、IC部は8KB程度の記憶容量を有し、記憶したデータは書換可能であるが、守秘性が保たれるという特徴を有している。

【0003】 従って、光記録部には画像のような大容量のデータや、書換えの必要のないものあるいは、書き換えられると困る個人用ID等の情報、IC部には書換える必要なディレクトリ情報や、秘密性の高い個人情報

記録されている。

【0004】 図8はこのカードの構成を示す図であり、光ICカード1は例えばその長手方向に帯状の光記録部2を有し、その光記録部2を外れた部分に、この例では光記録部2の上側にIC部3を有している。光記録部2の一部分をその右側に拡大して示しており、長手方向に設けられた細い帯状のトラッキングトラック2aに挟まれた帯状のエリアがデータトラック2bとなっており、そのデータトラック2bの長手方向中心部付近に、一列に配列された複数のビット2cが設けられている。

【0005】 ビット2cの記録再生方法は光ディスク装置等で公知の方法を用いており、また本発明に直接関係しないので記載を省略する。

【0006】 図9はビット5の記録状態を示す図であり、仮想的なビットセル2dの中央にビット2cがあればデータの「1」を示し、ビット2cがなければ「0」を示すようになっている。また、隣あったデータが「0」のときはその境界にセルフクロック用のビットを置くようにしている。

【0007】 図9の例では「01000001」のデータであり、アスキーコードで記録された情報であれば、「A」を示すことになる。

【0008】

【発明が解決しようとする課題】 しかしながら、このようにして記録した光カードは顕微鏡を使用すればビットの配列状態を読み取ることができるので、守秘性を要求されるデータは記録できないと言う課題を有していた。

【0009】 本発明はこのような状況に鑑みてなされたもので、守秘性を要求されるデータも光カードに記録できるようにしたものである。

【0010】

【課題を解決するための手段】 このような課題を解決するために請求項1に記載の光ICカードを使用した情報記録再生システムにおいて、光ICカードの光記録部に記録再生する際の暗号化の鍵をそのカードのIC部に持つことを特徴とする。

【0011】 請求項2に記載の光ICカードを使用した情報記録再生システムは、請求項1に記載の情報記録再生システムにおいて、暗号化の鍵をその光ICカードをアクセスする情報記録再生装置内に持つことを特徴とする。

【0012】 請求項3に記載の光ICカードを使用した情報記録再生システムは、請求項1または請求項2に記載の情報記録再生システムにおいて、光ICカード内の暗号化鍵と同じ暗号化鍵をアプリケーション提供者側のシステムに有することを特徴とする。

【0013】 請求項4に記載の光ICカードを使用した情報記録再生システムは、請求項1乃至請求項3に記載の情報記録再生システムにおいて、光記録部にセキュリティレベルを持ち、そのセキュリティレベルのうち少な

くとも一部は情報を記憶する光 I C カードに有する暗号化鍵とは別の鍵によってのみ再生できることを特徴とする。

【0014】請求項5に記載の光 I C カードを使用した情報記録再生システムは、請求項4に記載の情報記録再生システムにおいて、セキュリティレベルの一部をアクセスする別の鍵が I C カードに記憶されていることを特徴とする。

【0015】請求項6に記載の光 I C カードを使用した情報記録再生システムは、請求項4に記載の情報記録再生システムにおいて、セキュリティレベルの一部をアクセスする別の鍵が受動的な外部記憶メディアに記録されていることを特徴とする。

【0016】請求項7に記載の光 I C カードを使用した情報記録再生システムは、請求項4に記載の情報記録再生システムにおいて、セキュリティレベルの一部をアクセスする別の鍵が光カードまたは情報の記録される光 I C カードとは別の光 I C カードであることを特徴とする。

【0017】

【作用】請求項1に記載の光 I C カードを使用した情報記録再生システムは、光 I C カードの I C 部に記憶されている鍵によってその光 I C カードに記録される情報が暗号化され、またその鍵を使用して読出しが行われる。

【0018】請求項2に記載の I C 光カードを使用した情報記録再生システムは、請求項1に記載の情報記録再生システムにおいて、その光 I C カードに対して情報をアクセスする情報記録装置内に記憶された鍵によって光 I C カードに記録される情報が暗号化され、またその鍵を使用して記録された情報の読出しが行われる。

【0019】請求項3に記載の光 I C カードを使用した情報記録再生システムは、請求項1または2に記載の情報記録再生システムにおいて、光 I C カードへの情報暗号化が光アプリケーション提供者側システムに記憶された暗号化鍵で行われ、その暗号化鍵は光 I C カード内の暗号化鍵と同じ暗号化鍵が使用される。

【0020】請求項4に記載の光 I C カードを使用した情報記録再生システムは、請求項1乃至請求項3に記載の情報記録再生システムにおいて、光記録部にセキュリティレベルを持ち、そのセキュリティレベルのうち少なくとも一部は情報を記憶する光 I C カードに有する暗号化鍵とは別の鍵によってのみ再生される。

【0021】請求項5に記載の光 I C カードを使用した情報記録再生システムは、請求項4に記載の情報記録再生システムにおいて、セキュリティレベルの一部が I C カードに記録された別の鍵によってアクセスされる。

【0022】請求項6に記載の光 I C カードを使用した情報記録再生システムは、請求項4に記載の情報記録再生システムにおいて、セキュリティレベルの一部が受動的な外部記憶メディアに記録された別の鍵によってアクセ

スされる。

【0023】請求項7に記載の光 I C カードを使用した情報記録再生システムは、請求項4に記載の情報記録再生システムにおいて、セキュリティレベルの一部が光カードまたは情報が記録される光 I C カードとは別の光 I C カードに記録された別の鍵によってアクセスされる。

【0024】

【実施例】図1は本発明を適用した装置の一実施例を示す構成図であり、パーソナルコンピュータ4はその内部にアプリケーションプログラムおよび光 I C カードリーダライタのコントロールプログラムが収納されている。そしてパーソナルコンピュータ4に光 I C カードリーダライタ5接続されている。

【0025】この I C カードリーダライタ5は例えば光 I C カード1が着脱自在に挿入できるように構成されている。

【0026】図2はこのように構成された装置による情報の暗号化および復号化の流れを示す図であり、先ずステップ100に示すように記録する情報をパーソナルコンピュータ4から光 I C リーダライタ5を経由して光 I C カード1の I C 部3に入力する。

【0027】そして、ステップ101に示すように光 I C カード1の内部で暗号化し、その結果得られた情報をステップ102に示すように光 I C カードリーダライタ5に出力し、ステップ103に示すように、暗号化された情報を光記録部2に書き込む。

【0028】このとき情報の暗号化は光 I C カード1内に有する I C 部3の秘密の鍵によって行われ、 I C 部3内の鍵は外部から覗くことができないものであるため、暗号化された情報は鍵無しでは解読できない。

【0029】光 I C カード1の所有者はこの状態でカードを所持するが、この鍵が何であるかは知らないため、光記録部2に記録されている情報をビット列としては解読できても、情報そのものはわからない。

【0030】光 I C カード1に記録されたデータの読み取りはステップ104において光 I C カード1を光 I C カードリーダライタ5に挿入し、パーソナルコンピュータ4によって読み取りを行う。そしてステップ105において読み取られた情報を I C 部3に入力し、そこで鍵を用いてステップ106に示すように復号を行い、ステップ107においてパーソナルコンピュータ4に出力表示する。

【0031】図3は暗号化の具体例を示したものであり、記録する情報が仮にアルファベットの「A」であるとき、ビット列で「d」（01000001）と表される。暗号化の鍵として8ビットの任意のビット列、例えば「K」（00011011）を与えると暗号化は「d」と「K」のエクスクルーシブオア（XOR）を取ることによって行われる。

【0032】その結果のデータ「D」は（010110

10

20

30

40

50

5

10) となり、情報としてはアルファベットの大文字の「Z」を表すことになる。光ICカード1にはこの「Z」が書き込まれるため、元の情報「A」とは異なり、顕微鏡等で光ICカード1の可視情報を読み取っただけでは元のデータが「A」であることがわからない。復号は再生されたデータ「D」の(01011010)と暗号「K」の(00011011)のイクスクリューブオアをとることで、d(01000001)つまり、元の情報「A」を得ることができる。

【0033】このように、光ICカード1に記録される情報は元の情報と異なり、また暗号化するときの鍵はIC部3の内部にあって外部に出てくることがないため、暗号化の鍵を知らないものにとっては記録されている情報が何であるかを解読することはできない。

【0034】この例では簡単のために8ビットの鍵を使用した。ビット数を増やせばよりセキュリティを上げることができる。また、DES(Data Encryption Standard)のような方法を使用すると更にセキュリティを上げることができる。

【0035】このようにIC部3に暗号化の鍵を持たせることによってセキュリティを上げることができるが、万一このIC部が破損した場合、光記録部2に記録されている情報を解読できなくなってしまう、情報が失われることになる。

【0036】この場合、光ICカードリーダーダライタ5内に光ICカード1のIC部3に持つものと同じ鍵を持っていると、このような事故の際も情報が解読できなくなってしまうことはない。また、この場合は不正な光ICカードリーダーダライタによるIC部3へのアクセスを防止できる。

【0037】例えば今までに説明した例ではIC部3に与える情報は光ICカード1から読出した情報をそのまま与え、それを暗号化しているが、図3に示すような単純な鍵を使用すると、その入力と出力の関係で、何回か繰り返すうちに鍵が解読される可能性がある。従ってこのアプリケーション用ではない、他のリーダーダライタを用いれば鍵が解読される恐れがある。

【0038】しかし、光ICカードリーダーダライタ5の内部に光ICカード1の内部にあるのと同じ鍵があるところのような不正な解読を防止できる。また、IC部3が破損しても迅速にデータの再生が行える。

【0039】図4は更にセキュリティを向上させる場合の例であり、アプリケーション提供者システム6と端末システム7を通信回線8によって結んだものであり、アプリケーション提供者システム6は光カードリーダーダライタ6a、ターミナル6b、CPU6cから構成される。端末システム7はパーソナルコンピュータ7a、光ICカードリーダーダライタ7bから構成されている。

【0040】そしてユーザは光ICカード1を光ICカードリーダーダライタ7bに挿入することにより、そこで読

6

み取られたデータはアプリケーション側提供者システム6に送られそこで管理され、管理された結果が端末システム7に返送され、光ICカード1に書き込まれる。

【0041】この場合は、アプリケーション提供者システム6にIC部3と同じ鍵を持たせることにより、通信回線8および端末システム7には暗号化した情報しか現れない。もちろん更にICカードリーダーダライタ6aに同じ鍵があっても良い。

【0042】このような例の中で、図5に示すように、光ICカード1の中にセキュリティレベル記録領域9を設け、その領域を秘密でない情報の領域9a、端末システム7により読み取れる領域9b、アプリケーション提供者のみ読み取れる領域9cに分けている。このようにすると守秘性が高く、かつ広域で迅速なサービスが提供できるシステムを構成できる。

【0043】このような光ICカードが破損した場合、アプリケーション提供者にのみ読み取れる領域9cはアプリケーション提供者に光ICカードを返却しなければ内容がわからないが、それだけに高い守秘性が保たれる。

【0044】アプリケーション提供者側システム6を持つ場合、図6に示すようにアプリケーション提供者側システム6にICカードリーダーダライタ6dを設け、管理用ICカード6eで鍵の管理を行うと、大量の鍵を安全に管理することができる。

【0045】例えば64Kビットの容量を持つICカードを使うと、64ビットの鍵を1000個、すなわち1000枚の光ICカードの鍵を管理できる。このような構成にすれば例えば顧客種別の管理ができ、また鍵を変更する際も、対応する一つの鍵を変更するだけで可能である。

【0046】このICカードの代わりに受動的な外部記憶メディア、例えばハードディスクや光磁気ディスクあるいは、フロッピーディスク等を使用すると安全性は多少低下するが、更に大量の鍵を容易に管理できる。また、記憶容量が大きいと、長い鍵すなわちビット数の大きな鍵が使用できる。

【0047】管理用のカード6eに光カードや、光ICカードを使用すると、一つのセクタに記録できる記憶容量が実際に使用される光ICカードのセクタサイズと等しくするため、一つのセクタ長の鍵を使った場合、効率よく管理できる。更に、管理用光ICカードあるいは光カードの場合、図7に示すようにセクタ毎にユーザを変えて記録でき、記録する際に暗号化して記録するため、更に安全である。

【0048】以上のような鍵の管理はアプリケーション提供者システムだけでなく、端末システムにあっても、あるいは端末側だけにあっても良い。また、端末システムそのものがアプリケーション提供者になるときは以上に述べた鍵の管理がそのまま端末システム上に適用でき

30

40

50

る。

【0049】

【発明の効果】以上説明したように本発明は暗号化鍵を使用して光 I C カードに記録する情報を暗号化して記録再生するようにしたので、光 I C カードに記録された情報を読取ってもそれだけでは真の情報がわからないので守秘性が保たれるという効果を有する。

【図面の簡単な説明】

【図 1】本発明の一実施例の構成を示す構成図である。

【図 2】図 1 の装置の動作を説明するフローチャートである。

【図 3】暗号化の一実施例を示す図である。

【図 4】第 2 の実施例の構成を示す構成図である。

【図 5】光 I C カード内のセキュリティレベルを説明するための図である。

【図 6】第 3 の実施例の構成を示す構成図である。

【図 7】管理用光カードに記録されるデータの配列を説明するための図である。

【図 8】従来の光カードを拡大した構成を示す図であ

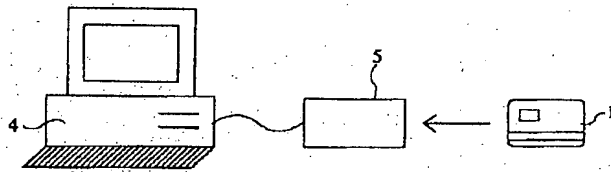
る。

【図 9】情報とビットとの関係を示す図である。

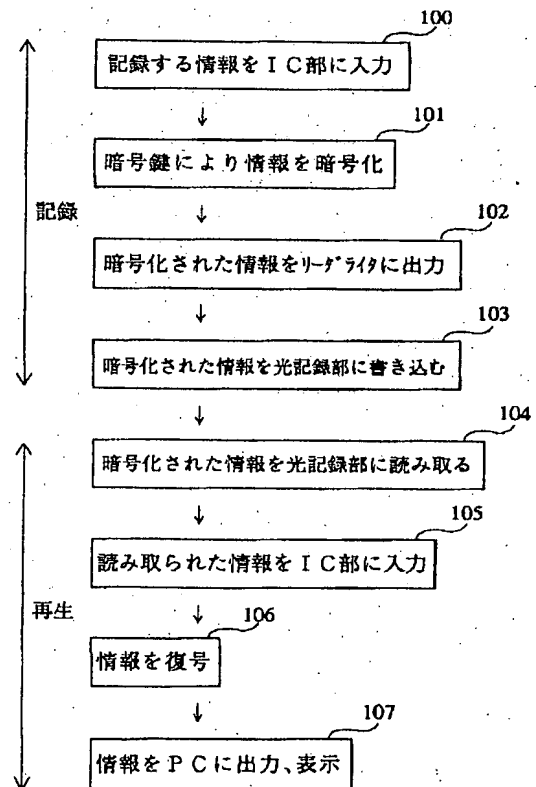
【符号の説明】

- 1 光 I C カード
- 2 光記録部
- 2 a トラッキングトラック
- 2 b データトラック
- 2 c ビット
- 2 d ビットセル
- 3 I C 部
- 4, 7 a パーソナルコンピュータ
- 5, 7 b 光 I C カードリーダライタ
- 6 アプリケーション提供者システム
- 6 a 光カードリーダライタ
- 6 b ターミナル
- 6 d I C カードリーダライタ
- 6 e I C カード
- 7 端末システム
- 8 通信回線
- 9 セキュリティレベル記録領域

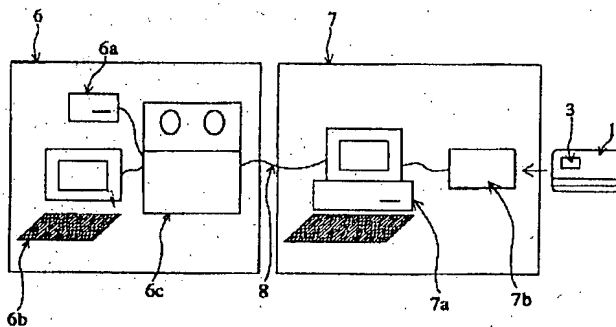
【図 1】



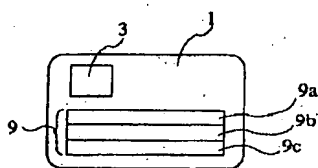
【図 2】



【図 4】



【図 5】



【図3】

情報 "A" d(01000001)
 鍵 K(00011011)
 暗号化 d XOR K=D(01011010)

$$\left[\begin{array}{r} d(01000001) \\ \text{XOR } K(00011011) \\ \hline D(01011010) \end{array} \right]$$

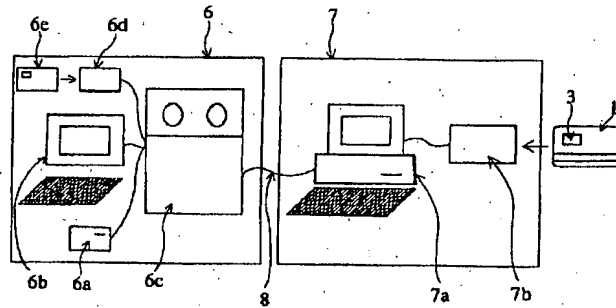
暗号化後情報 "Z" D(01011010)

復号 D XOR K=d(01000001)

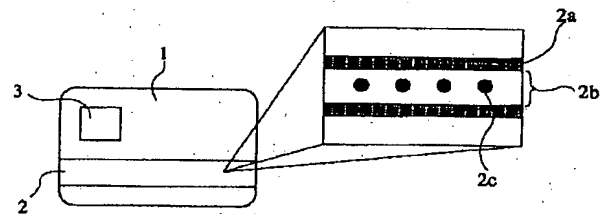
$$\begin{array}{r} D(01011010) \\ \text{XOR } K(00011011) \\ \hline d(01000001) \end{array}$$

復号化後情報 "A" d(01000001)

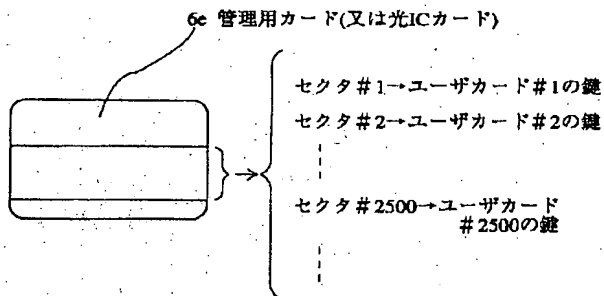
【図6】



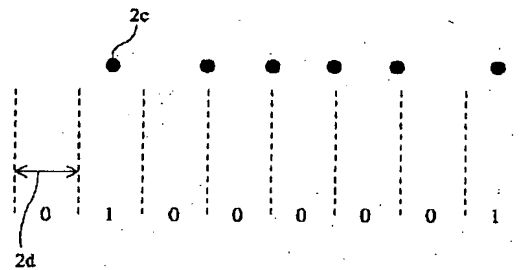
【図8】



【図7】



【図9】



フロントページの続き

(51) Int. Cl.⁵
 G 1 1 B 20/10

識別記号 庁内整理番号
 H 7923-5D

F I

技術表示箇所